AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of managing a communication with a mobile device over a network, comprising:

receiving a request from the mobile device, wherein the request includes associated information and further receiving a gateway group identifier for a carrier gateway that is associated with the mobile device request;

automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information, and based on:

using the gateway group identifier, determining if the carrier gateway is trustable above a defined level;

using the associated information, determining a capability of the mobile device, including determining if the mobile device is enabled to accept a cookie, and determining if the mobile device is enabled to interact with a Uniform Resource Locator (URL);

using the associated information, determining if a trusted mobile device identifier associated with the mobile device is received;

if the trusted mobile device identifier associated with the mobile device is received and the carrier gateway is trustable above the defined level, then determining at least a first level of trust associated with the mobile device;

if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and

if the mobile device is enabled to interact with a URL ~~Uniform Resource Locator (URL)~~, then determining at least a third level of trust associated with the mobile device; and

determining at least one device signature for the mobile device based on the at least one level of trust from the plurality of different levels of trust, and independent of user authentication, the at least one device signature being useable to enable the mobile device to perform an action over the network associated with the request.

2. (Previously Presented) The method of Claim 1, wherein the gateway group identifier is obtained from a header of a network packet associated with the carrier gateway.

3. (Original) The method of Claim 1, wherein the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie.

4. (Previously Presented) The method of Claim 3, wherein the associated information further comprises a subscription identifier.

5. (Previously Presented) The method of Claim 1, wherein the method further comprises:

automatically determining a second device signature based on the second level of trust, wherein the second device signature comprises a hash of at least a cookie, the gateway group identifier and a user agent identifier obtainable from the associated information.

6. (Original) The method of Claim 1, wherein the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

7. (Previously Presented) The method of Claim 1, wherein if a trusted mobile device identifier associated with the mobile device is received, further comprises:

determining a level of trust of the carrier gateway associated with the mobile device based on a received subscription identifier and the gateway group identifier in the associated information; and

if the determined level of trust for the carrier gateway is above a determined level, trusting the received mobile device identifier, and

if the mobile device identifier is trusted, then enabling the determination of at least the first level of trust associated with the mobile device: and

if the mobile device identifier is untrusted, then inhibiting the determination of the at least first level of trust associated with the mobile device.

8. (Canceled)

9. (Previously Presented) The method of Claim 1, wherein the mobile device identifier is at least one of a mobile identification number (MIN), an Electronic Serial Number (ESN), application serial number, or a mobile telephone number.

10. (Previously Presented) The method of Claim 1, wherein determining at least one device signature further comprises:

if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp.

11. (Previously Presented) The method of Claim 1, wherein determining at least one device signature further comprises:

if the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp.

12. (Previously Presented) The method of Claim 1, wherein determining at least one device signature further comprises:

if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

13. (Original) The method of Claim 12, wherein determining the third tier device signature further comprises including the third tier device signature in a munged URL.

14. (Original) The method of Claim 1, wherein determining at least one device signature further comprises employing a hash function selected from at least one of a Message Digest, a Secure Hash Algorithm (SHA), Digital Encryption Standard (DES), triple-DES, Hash of Variable Length (NAVAL), RIPEMD, and Tiger hash function.

15. (Original) The method of Claim 1, further comprising expiring the at least one device signature based, in part, on a predetermined period of time associated with each of the at least one device signature.

16. (Original) The method of Claim 1, further comprising:

if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

17. (Original) The method of claim 16, wherein determining if the expired device signature is to be rolled over further comprises evaluating at least one of a condition, event, change in an identifier indicating a grouping of the gateway, and a time.

18. (Currently Amended) A client adapted for a mobile device to communicate with a server over a network, the client being configured to perform actions, comprising:

sending a request to the server for content, wherein the request includes an identifier associated with a user agent, and wherein a carrier gateway associated with the request further provides a gateway group identifier; and

receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust determined from a plurality of different trust levels, and is independent of user authentication, the at least one level of trust being determined based on:

determining at least a default level of trust,

determining if the carrier gateway is trustable based on the gateway group identifier,

if a trusted mobile device identifier associated with the mobile device is received and the carrier gateway is determined to be trustable, then determining at least a first level of trust associated with the mobile device;

determining if the mobile device is enable to accept a cookie, and if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and

determining if the mobile device is enable to interact with a Uniform Resource Locator (URL), and if the mobile device is enabled to interact with the URL ~~a Uniform Resource Locator (URL)~~, then determining at least a third level of trust associated with the mobile device.

19. (Previously Presented) The client of Claim 18, wherein the client is configured to perform actions, further comprising:

providing the mobile device identifier based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

20. (Previously Presented) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on the first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, the user agent identifier, and a time stamp.

21. (Previously Presented) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on the second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, the user agent identifier, and a time stamp.

22. (Previously Presented) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on the third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

23. (Previously Presented) The client of Claim 18, wherein sending the request further comprises sending the request to the carrier gateway, wherein the carrier gateway is configured to perform actions, comprising:

modifying the request to include at least one of a subscription identifier associated with the mobile device, and the gateway identifier;

forwarding the modified request to the server; and

receiving the at least one device signature from the server; and forwarding the at least one device signature to the mobile device.

24. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature.

25. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, associating a munged Uniform Resource Locator (URL) with the at least one device signature.

26. (Currently Amended) A server for managing a communication with a mobile device over a network, comprising:

a transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device; and

a transcoder that is configured to perform actions, including:

receiving the request from the mobile device, wherein the request includes associated information;

receiving, from a carrier gateway associated with the request from the mobile device, a gateway group identifier for the carrier gateway;

automatically determining at least one level of trust from a plurality of different trust levels based, in part, on the associated information and further based on:

if a trusted mobile device identifier associated with the mobile device is received and the carrier gateway is determined to be trustable based on the gateway group identifier, then determining at least a first level of trust associated with the mobile device;

determining if the mobile device is enable to accept a cookie, and if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device: and

determining if the mobile device is enable to interact with a Uniform Resource Locator (URL), and if the mobile device is enabled to interact with the URL ~~a Uniform Resource Locator (URL)~~, then determining at least a third level of trust associated with the mobile device; and

determining the at least one device signature for the mobile device based on the at least one level of trust of the plurality of different trust levels, wherein the at least one device signature is independent of user authentication.

27. (Original) The server of Claim 26, wherein the transcoder is configured to perform further action, comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

28. (Previously Presented) The server of Claim 26, wherein determining the at least one device signature further comprises:

if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp.

29. (Previously Presented) The server of Claim 26, wherein determining the at least one device signature further comprises:

if the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp.

30. (Previously Presented) The server of Claim 26, wherein determining the at least one device signature further comprises:

if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

31. (Previously Presented) The server of Claim 26, wherein determining the at least one level of trust further comprises determining the first level of trust based at least one of the gateway group identifier, a subscription identifier, a user agent, and a security level associated with the request from the mobile device to determine if the mobile device identifier is trusted.

32. (Previously Presented) The server of Claim 26, wherein determining the at least one level of trust further comprises determining the second level of trust based at least one of the gateway identifier, and a user agent

33. (Canceled)

34. (Original) The server of claim 26, wherein the transcoder is configured to perform further actions, comprising:

determining if at least one device signature has expired device, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

35. (Currently Amended) A system for managing a communication with a mobile device over a network comprising:

the mobile device configured to provide information associated with the mobile device; and

a server, coupled to a carrier gateway, that is configured to receive the associated information and to perform actions, including:

automatically determining at least two different levels of trust from a plurality of different levels of trust based, in part, on the associated information, wherein the at least two different levels of trust are based on:

if a trusted mobile device identifier associated with the mobile device is received, a [[a]] gateway group identifier associated with the carrier gateway is determined to be trustable, then determining at least a first level of trust associated with the mobile device, and

determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a Uniform Resource Locator (URL); and

initially determining at least two different device signatures for the mobile device each of the two devices signatures being based on a different one of the at least two different levels of trust, wherein the at least two device signatures are each determined independent of user authentication.

36. (Previously Presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp.

37. (Previously Presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp.

38. (Previously Presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 3 device signature based, in part, on a hash of

at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

39. (Original) The system of Claim 38, wherein the tier 3 device signature is provided to the mobile device through a munged URL.

40. (Previously Presented) The system of Claim 35, further comprising:

the carrier gateway, coupled to the mobile device, that is configured to receive the associated information, and provide the associated information and gateway information, including the gateway group identifier, related to the carrier gateway.

41. (Currently Amended) A computer readable storage medium for communicating with a mobile device, the computer readable storage medium having computer executable instructions stored thereon that when installed into a computing device enable the computing device to perform actions, comprising:

receiving a request from the mobile device, wherein the request includes associated information and further receiving a gateway group identifier associated with a carrier gateway for the mobile device request; and

sending at least one device signature to the mobile device based on at least one level of trust determined from a plurality of different levels of trust that is determined, in part, using the associated information, wherein the at least one level of trust is based on:

if a trusted mobile device identifier associated with the mobile device is received and the carrier gateway is determined to be trustable based on the gateway group identifier above a threshold, then determining at least a first level of trust associated with the mobile device; and

determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a Uniform Resource Locator (URL), and wherein the at least one device signature is determined independent of user authentication.

42. (Previously Presented) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp.

43. (Previously Presented) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if the other second level of trust is determined, determining another second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp.

44. (Previously Presented) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if the other level of trust is determined, determining another tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time

45. (Currently Amended) An apparatus for communicating with a mobile device, comprising:

a means for receiving a request from a mobile device, wherein the request includes associated information, wherein the associated information indicates a capability of the mobile device;

means for receiving a gateway group identifier associated with a carrier gateway for the request from the mobile device;

a means for automatically determining a plurality of different levels of trust based, in part, on the associated information, wherein at least one of the different levels of trust is based on an operational capability of the mobile device and if the carrier gateway is trustable above a threshold based on the gateway group identifier, and wherein another one of the different levels of trust is based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a Uniform Resource Locator (URL); and

a means for determining a plurality of different device signatures for the mobile device based, in part, on the determined plurality of different levels of trust, and independent of user authentication.